EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ramin Aghevli (Reg No. 43,462) on 1/21/2010.

The application has been amended as follows:

1. (Currently Amended) A method comprising: performing modular exponentiation in a cryptographic computation such that memory accesses are independent of the numerical value of the exponent, wherein said performing modular exponentiation is to comprise replacing a conditional multiplication operation with an unconditional multiplication operation and the unconditional multiplication operation is to be based on an obscuring factor; and determining the obscuring factor for each bit of the exponent by adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity comprising a message minus one.

24. (Currently Amended) An article comprising: a non-transitory storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for obscuring cryptographic computations by performing modular exponentiation of an exponent in a cryptographic

computation such that memory accesses are independent of the numerical value of the exponent, wherein a current obscuring factor is to be determined by adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity to comprise a message minus one.

27. (Currently Amended) An article comprising: a non-transitory storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for obscuring cryptographic computations by performing modular exponentiation of an exponent in a cryptographic computation such that memory accesses are independent of the exponent bit pattern, the instructions causing setting an intermediate value to a message; and for each bit i in the exponent, setting the intermediate value to the intermediate value multiplied by the intermediate value mod a modulus, wherein the modulus comprises a product of two prime numbers, determining a current obscuring factor using the i'th bit of the exponent, and setting the intermediate value to the intermediate value multiplied by the current obscuring factor mod the modulus, wherein determining the current obscuring factor is to comprise adding one to a result of multiplying a quantity by a selected bit of the exponent, the quantity to comprise the message minus one.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SIMON KANAAN whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SIMON KANAAN/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432